DOD Privacy Impact Assessment (PIA)

1. Name of MACOM / DA Staff Proponent (APMS Sub Organization Name)

U. S. Army, Office of the Assistant G-1 for Civilian Personnel

2. Name of Information Technology (IT) System.

Civilian Forecasting System (CIVFORS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

550

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0690-200 DAPE, Department of the Army Civilian Personnel Systems

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 3013, Secretary of the Army
Army Regulation 690-200, General Personnel Provisions
Executive Order 9397

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of the system and components, and system backup)

The purpose of CIVFORS is to support the development and implementation of effective strategic workforce plans for the Department of Army civilian personnel. CIVFORS produces analytical information (to include forecasting) for input to policy formulations,

workforce planning, evaluation and personnel business process improvements. CIVFORS is in the operation and maintenance life cycle phase. The system contains information pertaining to Army civilian workforce personnel.

CIVFORS interfaces with the HQ Army Civilian Personnel Data System (HQ ACPERS) via a secure network connection. Users can access the CIVFORS system by use of a web browser. Web servers, application servers and database servers are located in Alexandria, Virginia.

Full database backups are run daily. System event logs are checked daily by the administrator / information assurance security officer. Tapes are stored at a commercial site in Atlanta, Georgia.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)

Information in identifiable form that will be collected includes: name, social security number (SSN), age, date of birth, gender, address, civilian type, race national origin code, clearance type, employee status, occupation code, pay grade, performance rating, occupational skills, educational information, dependent status, marital status and citizenship status. The source of the information is from HQ ACPERS (the Army civilian workforce database repository) via a secure network connection.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Information used by CIVFORS is extracted from HQ ACPERS (the Army civilian workforce database repository) via a secure network connection.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

The Government Accountability Office (GAO), through a series of reports has recommended to the Secretary of Defense that DoD and each service develop a personnel management system which will align human capital strategic plans with the overall mission of the Department of Defense (DoD). This system accomplishes that requirement for the Army. Information in identifiable form is collected and used by this system in direct support of these missions.

13. Describe how the information in identifiable form will be used (e.g. to verify exiting data, etc.).

Information in identifiable form will be used to derive statistical data and forecasting for input to policy formulations, workforce planning, evaluation and personnel business process improvements.

14. Describe whether the system derives or creates new data about individuals through aggregation.

The system does not derive or create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies).

Information will be available to authorized users with a need to know in order to perform official government duties. Information from this system is shared among the Army personnel community which consists of the Civilian Personnel Operations Centers, the Civilian Personnel Advisory Centers, Army Civilian Human Resources Agencies and U.S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Manpower Data Center, Defense Criminal Investigative Service, Under Secretary of Defense for Personnel & Readiness, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable for about themselves or to contest to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Information in identifiable form is not collected directly from the individual thus individuals are not given the opportunity to object to the collection of information in identifiable form about themselves or to contest the specific uses of the information in identifiable form. Individuals give implied consent to the use, collection and storage of their personally identifiable information when they initially provide information to Army civilian personnel systems.

17. Describe any information that is provided to and individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of the delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Information in identifiable form is not collected directly from the individual thus individuals are not provided a Privacy advisory by this system. Individuals are implicitly consenting to the capture and use of this information when employed by the Department of Army civilian workforce when they are initially furnished a Privacy advisory.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secure facilities. These facilities have armed guards that verify the credentials (appropriate DoD building/identification badge) of all employees and login all visitors including, vendors and maintenance. Users of this system include the Army Civilian Personnelists and administrative and technical support personnel. Users accessing government computer information are required to undergo and receive at a minimum automatic data processing / information technology (ADP/IT) level III background investigation. These users (both government and contractor) may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role. Users must enter appropriate user Identification and password before being authorized access to the resources. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, etc.). Additionally, all aspects of privacy, security, configuration, operations, data retention and disposal are documented to ensure privacy and security are consistently enforced and maintained. There is weekly monitoring of security events, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIGs). Files transferred across the internet/NIPRNET are encrypted.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program" November 11, 2004. If so, and a System of Records Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when the publication of the notice will occur.

The system requires a SORN and it is published.

20. Describe/evaluate any potential privacy risk regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate and privacy risks in providing individuals and opportunity to object/contest or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individual's privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Information is protected by user passwords, Common Access Card (CAC) access, firewalls, antivirus software and data-at-rest protection on portable laptops thus the level risk with these adopted security measures is minimal.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.